IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO. 5:10CR216
	)	
Plaintiff,	)	JUDGE LESLEY WELLS
	)	
v.	)	
	)	UNITED STATES OF AMERICA'S
MITCHELL L. FROST,	)	SENTENCING MEMORANDUM
	)	
Defendant.	)	

Now comes the United States of America, by its counsel Steven M. Dettelbach, United States Attorney, and Robert W. Kern, Assistant United States Attorney, and respectfully submits this memorandum setting forth the United States' position regarding the calculation of the applicable Sentencing Guidelines level and the sentencing factors set forth in Title18, U.S.C., Section 3553(a) relative to the imposition of sentence for the defendant, Mitchell L. Frost.

In summary, the United States submits that the Presentence Investigation Report properly calculates the Defendant's advisory Sentencing Guidelines range as 18-24 months of incarceration. However, based upon the seriousness of the offense, the defendant's failure to disclose all relevant financial information to the Probation Office during the Presentence Investigation, the defendant's continued activity in growing and use of marijuana, and his obvious lack of remorse, the Court should consider an upward departure or upward variance from that range, and that the Court should instead impose a sentence withing the advisory guidelines range of 27 -33 months, or higher.

I. BACKGROUND

On May 26, 2010, the defendant entered guilty pleas to both counts of a two count Information, charging violations of 18 U.S.C., Section 1030(a)(5)(A)(i) [Transmission of Harmful Computer Code or Commands with intent to Damage], and 18 U.S.C., Section 1029(a)(3) [Possession of 15 or more unauthorized access devices]. The Rule 11 plea agreement contains what the parties agree is the proper calculation of defendant's offense level under the advisory Sentencing Guidelines. Both parties, however, have reserved the right to seek departures and/or variances from that offense level. For the reasons set forth herein below, the government respectfully moves the Court for an upward departure and/or an upward variance,

and respectfully requests that the Court sentence the defendant within the range of 27-33 months, or higher.

The offense conduct is set forth in detail in the Presentence Investigation Report at paragraphs 9 through 23. At the time of this offense, the defendant was an undergraduate student at the University of Akron (hereinafter "UA"). On or about October 7, 2006, a network engineer at UA discovered unusual activity on the University's computer network stemming from the defendant's user account.

Further investigation revealed that the defendant was controlling other computers by means of "Bot Net Zombies"[1] on the Internet, which were computers

[1] The term "bot" is derived from the word "robot" and generally describes a computer program that performs some predefined function in an automated fashion. An Internet Relay Chat ("IRC") robot or "bot" is a program running as an IRC client that responds autonomously to commands sent to it by the IRC server. Whereas a typical IRC client application provides information to a human, an IRC bot receives commands, performs numerous functions, and provides information back to the IRC server without human interaction at the client level. Originally bots were used to provide interactive access to non-IRC resources. For example, a weather bot might look up weather information based upon a zip code provided to it by the IRC server. IRC users could query the weather bot and receive a response based upon the weather in the zip code provided. More recently, IRC bots have been adapted as a tool for malicious conduct via the Internet. The malicious bots are created by individuals (or groups) who scan the Internet looking for vulnerable computers, use an exploit to hack into the vulnerable computers, and then install malicious controlling software (known as malware or bot malware) on the hacked computers. Embedded in this malware is an address of an IRC server, a unique channel name, and any password required to gain access to that particular IRC channel. The infected computer then follows the command it has been given to seek out this IRC channel, join it, and await commands disseminated via the IRC channel.

Typical functions of a bot installed on an infected computer may include: (1) creation of a "back door" to the infected computer that will allow a malicious controller future access to, and complete control over the infected computer; (2) installation of a keystroke logger, allowing the malicious controller to intercept communications and all keystrokes of the user of the bot

located throughout the United States and in other countries which had been compromised. The defendant gained access to these other computers and obtained personal identifying information, including user names and passwords, for the computers compromised. The defendant, in turn, used the compromised computers to spread malicious software code (*i.e.*, "malware") to even more computers in order to compromise those computers and harvest even more data from them, and to utilize the compromised computers to launch multiple Distributed Denial of Service (DDoS)[2] attacks against certain Internet web sites.

The UA network engineer also became aware that the defendant was communicating with other individuals via Internet Relay Chat (IRC), and was discussing schemes to use stolen credit card information to purchase merchandise via the Internet, for delivery to various locations in exchange for cash payments to the defendant.

---

infected computer; (3) installation of other malware on the bot infected computer such as spyware; (4) capture and theft of personal identification and financial information, passwords or web-based e-mail and/or messenger account login information; and (5) capture and theft of software activation codes required to operate or run commercial software programs.

[2] A distributed denial of service or "DDoS" attack is designed to flood a computer system or network with an incapacitating volume of traffic in order to overwhelm the victim or target system, thereby shutting the computer system or network down. If the target system or network is serving as the host for an Internet web site, shutting down the system or network will, in turn, cause the Internet web site to shut down as well.

UA Police officers met with the defendant on October 25, 2006, regarding his activities. The defendant denied any knowledge of the aforementioned activities, and indicated that he was working for the FBI. The defendant refused to provide the UA police with a name for his "purported" contact at the FBI.

Thereafter, officials at UA contacted the Akron Office of the United States Secret Service concerning this matter. Secret Service agents reviewed computer logs and Internet Relay Chat logs provided by UA officials, which logs clearly reflected that the defendant was involved in the programming and distribution of malicious computer code, attacking and compromising remote computer systems, launching DDoS attacks, running botnets and was involved in credit card fraud activities, all while connected to the UA computer network.

Despite the defendant's claim that he knew nothing about such activity, the UA officials continued monitoring defendant's on-line activities. IRC chat logs captured from November 16, 2006, and December 13, 2006, for example contain numerous instances of defendant discussing control of the botnet, launching attacks against computer systems, "phishing" (*i.e.*, on-line activity to fraudulently obtain identity or financial records), posting information or data stolen from compromised computer systems, discussing placing orders with stolen credit card information and shipment of merchandise so obtained, discussing "taking down"

the university network if his Internet access was turned off again, and also discussion concerning the growing, selling and use of marijuana.[3] The defendant also discussed meeting with the UA police in October of 2006.

On November 28, 2006, UA officials logged another IRC chat session where the defendant stated that following his encounter with UA police in October, the defendant feared the police would "raid" his room, so he copied his so-called "bad files" onto a DVD+R disk and hid it above the ceiling tiles outside of his room in the dormitory hallway. At the request of UA police, the maintenance department checked above the ceiling tiles in the hallway outside the defendant's dorm room and found a DVD+R disk which was turned over to the police. (Once formatted and recorded, the data contained on a DVD+R disk is "locked" and cannot be subsequently altered, modified, added to or deleted).

UA network administrators continued to monitor the defendant's Internet activity, and discovered that in March 2007, the defendant was bragging in IRC chat sessions about DDoS attacks he had launched against the Internet websites of billoreilly.com, anncoulter.com and joinrudy2008.com. University logs were examined and revealed that between March 7, 2007, @ 8:21 p.m. and March 12,

[3] As discussed below, defendant's involvement with the growing and use of marijuana apparently did not cease when he left the University of Akron in April of 2007.

2007, @ 12:47 a.m., the defendant had initiated or "launched" attacks against these specific web sites at least 11 times. As a result of said attacks, these web sites were knocked off-line for periods of time and the owners of the sites billoreilly.com and anncounter.com have reported that losses greater than $5,000 were incurred. Billoreilly.com has submitted a victim impact statement to the Probation Office which claims losses totaling $41,000 as a result of the defendant's actions. These include $21,500 in lost revenue and compensated site memberships, $15,000 in Internet connectivity or bandwidth charges incurred as a result of these attacks, and lost employee time of $4,500 in responding to and addressing the disruption caused by the defendant's conduct.[4]

Additionally, on March 14, 2007, UA computer logs revealed that defendant had launched a denial of service attack against a computer game server located in the UA library, which had the apparent unintended result of knocking the entire UA computer network off-line for approximately 8 ½ hours, thereby preventing all students, faculity and other staff members from accessing the UA computer network during this time. UA officials are expected to submit a separate victim

[4] Billoreilly.com's victim impact statement also indicates that an additional $40,000 in hardware upgrades were required following the attacks initiated by the defendant. Because the hardware was an "upgrade" and not simply equipment to restore the computer system to its previous, albeit vulnerable state, it is unclear whether this amount may be included in a restitution order.

impact statement concerning the effects of this outage.

A federal search warrant was obtained on March 22, 2007, for the DVD+R disk which the defendant hid above the ceiling tiles. Multiple files and folders on the DVD+R contained illegally obtained credit card information, including the names, addresses, credit card account numbers, card holders' dates of birth, social security account numbers, PINs, and other information pertaining to bank accounts which may have been linked to the credit card. Additionally, the DVD+R disk contained a chat session between the defendant and another individual on August 5, 2006, during which session defendant provided credit card information from two separate credit card accounts to the other individual, in exchange for a Western Union money order which the other individual was instructed to mail to the defendant's home address in Bellevue, Ohio.

On April 7, 2007, a federal search warrant was executed at the defendant's UA dormitory room in Gallucci Hall. Seized during the execution of the search warrant were the defendant's computer, digital camera, multiple CDs and DVDs, memory cards, thumb drives, a cell phone, an i-Pod and an external hard drive.

Subsequent examination of the computer and electronic storage media seized from the defendant's dorm room revealed numerous IRC chat logs in which the defendant and others discussed how to steal and use credit card information

and make on-line purchases. Also found on the defendant's computer was stolen credit card account information for approximately 136 credit card accounts, user log-on ids and passwords for approximately 2,923 separate users, and computer log information which indicated that the defendant had launched numerous dedicated denial of service (DDoS) attacks from his computer, including the attacks against billoreilly.com, anncoulter.com and joinrudy2008.com.

Title 18, United States Code, Section 1029(e)(1) defines "access device" as any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

Title 18, United States Code, Section 1029(e)(3) defines "unauthorized access device" as any access device that is lost, stolen, expired, revoked, cancelled or obtained with the intent to defraud.

Here, the access devices in question are the 136 stolen credit card account numbers and PINs, and the 2,923 computer user log-ons and passwords which defendant possessed and used in connection with these offenses.

Microsoft Corporation of Redmond, Washington, monitors, tracks and maintains data with respect to certain suspicious or illegal activities on the Internet. In response to a federal grand jury subpoena served upon Microsoft in April 2007, logs and other information concerning the defendant's activities were provided to the U.S. Secret Service. Specifically, during the two year period prior to the service of the subpoena, Microsoft had discovered the defendant in the IRC channels scanning computer systems and networks in various ranges of IP addresses, looking for vulerable computers to compromise. Microsoft was able to capture the various command and control servers the defendant was utilizing during this time.

Specifically, Microsoft captured information relating to fourteen (14) denial of service attacks the defendant launched through five different command and control channels. The logs show the defendant downloading commands, updating the "bots" and getting the "bots" to download and install malware. Ten of the targets of these 14 denial of service attacks logged by Microsoft were located in the United States, two were in Canada, one in Germany and one was in Denmark. Microsoft was unable to provide any information concerning potential or possible losses connected with these 14 attacks.

The UA network logs, the Microsoft logs and the information and data found on the defendant's computer and other electronic storage media clearly establishes that the defendant was not merely a naive young college student with an inquisitive mind and a thirst for knowledge, but rather by the age of 19, the defendant was a serious, hard-core, malicious computer hacker who had the knowledge, tools and motivation to steal personal information, hack into computer systems and networks, create an army of "robot" zombie computers, and launch cyber attacks against numerous computer system and web sites.

Despite knowledge of the pending federal investigation, and now with the pending federal charges, defendant has continued to engage in questionable/illegal conduct. Furthermore, the government has recently become aware that the defendant failed to report to the Probation Officer preparing his Presentence Investigation certain questionable business/commercial activity he is conducting via an Internet website.

On July 13, 2010, undersigned counsel for the United States was notified by the FBI that Firelands Federal Credit Union of Bellevue, Ohio, had reported certain activity pertaining to the defendant. Specifically, the credit union reported that the defendant had sent frequent wire transfers of funds to China apparently to purchase "JWH." When questioned by credit union officials, the

defendant claimed to be selling the JWH as "Bonzai Fertilizer" via an Internet website he operates. Defendant's account also reflected over 168 debit (payment) transactions to UPS totaling $2,810.15 (presumably shipping costs incurred by defendant), and 56 Paypal credits (deposits) totaling $23,842.47 (from sales of JWH).

Paypal also separately reported activity by the defendant. Paypal indicated that between February 2010, and April 29, 2010, defendant's Paypay account received deposits of approximately $14,722.30 from the sale of JWH-018, a compound which is used as a substitute for marijuana. $12,144.93 of said funds had been withdrawn and deposited into defendant's account at Firelands Credit Union.

The domain name for the website (www.DISCOUNTJWH.com) is registered to Mitchell Frost, 1655 West Main Street, Bellevue, Ohio 44811, and the telephone number listed on the registration is the same number listed in the Presentence Report as the defendant's telephone number. The domain name www.DISCOUNTJWH.com was registered by the defendant on January 27, 2010. Review of the website reveals that quantities of JWH can be purchased from defendant ranging from 100mg for $10.00, up to 50 grams for $950.00. Photographs of mounds of white powder appear repeatedly throughout the website

pages. The contact information for "Sales & Support" lists the same telephone number as that listed in the PSR as the defendant's telephone number. Copies of the website's pages are attached hereto as Exhibit A.

According to open-source information available on the Internet, JWH-081 is an analgesic chemical which produces the same effects as THC in marijuana. The compound can be smoked like marijuana or burned as incense and inhaled into the lungs. It can also be ingested or consumed orally. The "high" which users experience is said to be far more intense than that experienced from smoking cannabis. Continued use or exposure to JWH may also produce dependence similar to that experienced from continued and prolonged cannabis use. Known side effects from use of JWH include hallucinations, agitation, elevated heart rates, vomiting, and other health effects. Additionally, JWH does not show up in routine drug tests which screen for marijuana usage.

It is anticipated that the defendant will claim that this activity should not be considered by the Court in fashioning an appropriate sentence in this case since JWH is not illegal in the State of Ohio; which is true.[5] Based upon the foregoing,

[5] It should be noted, however, that as of July 19, 2010, the substance had been banned in at least seven states (Alabama, Arkansas, Georgia, Kansas, Kentucky, North Dakota and Tennessee) and proposed legislation banning JWH was pending in seven other states (Florida, Illinois, Louisiana, Michigan, Missouri, New York and Utah). The substance has also been banned or is

however, it is clear that the defendant has been conducting a for-profit commercial business activity, and that he intentionally failed to report not only the activity, but also the income associated with the activity to the Probation Officer who prepared the defendant's Presentence Report. The fact that the activity involves the sale of a synthetic form of marijuana merely compounds the problem.

Additionally, the government has identified numerous postings on an Internet forum board made by the defendant, who was still using the same screen name "FrostAie" as recently as May 2010. The forum or discussion board is known as "grasscity.com" and focuses on various topics all related to marijuana or "grass."

Postings made by "FrostAie" between February 19, 2008, and May 26, 2010, are attached to this memorandum as Exhibit B. In these Internet postings, the defendant: (1) relates his futile attempts to submit a fraudulent urine sample for a work-related drug test; (2) discusses and exhibits photographs of his marijuana growing operation (both indoor and outdoor); (3) discusses his frustration with and opposition to law enforcement eradication efforts; (4) and

---

otherwise controlled in the Austria, Belarus, Canada, France, Ireland, Italy, Latvia, Poland, South Korea, Sweden, Estonia, Romania, Russia and the United Kingdom. The U.S. Drug Enforcement Administration labeled JWH a "drug or chemical of concern" in 2009.

boasts about knocking Bill O'Reilly.com off-line several years earlier (3 posts dated February 5, 2010; 1 post dated March 27, 2010).[6]

Based upon the foregoing, the United States respectfully submits that the Court should consider an upward departure from the Sentencing Guidelines level set forth in the Presentence Report, and should sentence the defendant within the range of 27-33 months, or higher.

II. APPLICABLE LEGAL STANDARDS

Any sentencing determination must begin with the calculation of the defendant's total offense level under the Sentencing Guidelines. Although the Supreme Court has declared the Guidelines to be advisory, it has also stated that "[a]s a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark." *Gall v. United States*, 128 S. Ct. 586, 596 (2007). The Sixth Circuit adheres to this view, holding that sentencing determinations should begin with a calculation of the appropriate Guidelines range. The Guidelines then serve as an element to be considered along with the other sentencing factors set forth in 18 U.S.C., Section 3553(a). *See United States v. Collington*, 461 F.3d 805, 807 (6th Cir. 2006).

[6] In one posting, dated February 5, 2010, the defendant stated "the day i got bills website down and made him rage was the greatest day of my life period. . . those were the golden days like I always like to say 'We Distort You Decide'" (sic)

The Sentencing Guidelines, therefore, remain an indispensable resource for assuring appropriate and uniform punishment for federal criminal offenses. While, to be sure, "[i]n accord with 18 U.S.C., §3553(a), the Guidelines, formerly mandatory, now serve as one factor amoung several courts must consider in determining an appropriate sentence," *Kimbrough v. United States*, 128 S. Ct. 558, 574 (2007), it remains the case that "the Commission fills an important role: It has the capacity courts lack to 'base its determinations on empirical data and national experience, guided by a professional staff with appropriate expertise,'" *Id.* at 574 (quoting *United States v. Pruitt*, 502 F.3d 1154, 1171 (10th Cir. 2007) (McConnell, J., concurring)).

In addition to the Guidelines, this Court must also consider all of the sentencing considerations set forth in 18 U.S.C., Section 3553(a). Those factors include: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (3) the need to afford adequate deterrence to criminal conduct, and to protect the public from further crimes of the defendant; (4) the need to provide the defendant with educational or vocational training, medical care, or other correctional treatment in the most effective manner; (5) the

guidelines and policy statements issued by the Sentencing Commission; (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and (7) the need to provide restitution to any victims of the offense. 18 U.S.C., Section 3553(a).

III. SENTENCING GUIDELINES COMPUTATION

The plea agreement in this case contains stipulations of fact which resulted in an Adjusted Offense Level of 15: Sentencing Guidelines §2B1.1 provides for a base offense level of 6 for the offenses charged; Guidelines §2B1.1(b)(1)(D) provides for a 6 level increase because there was a stipulated loss greater than $30,000, but less than $70,000; Guidelines §2B1.1(b)(10)(B)(i) provides for a 2 level increase because the offense involves the trafficking in access devices; Guidelines §2B1.1(b)(16)(A)(ii) provides for a four level increase because the offense involved a conviction under 18 U.S.C., §1030(a)(5)(A).

The plea agreement further provided that if the defendant continued to accept responsibility for his conduct, and did not violate the plea agreement or the terms and conditions of his bond, the government would request the third level under Guidelines Section 3E1.1(b) at the time of sentencing. The agreement stated that defendant understood that the Court will determine acceptance of responsibility based upon the defendant's overall conduct as of the date of

sentencing, and that if defendant received credit for all three levels of acceptance of responsibility, his Adjusted Offense Level will be 15.

Based upon the defendant's involvement in establishing an Internet website to sell JWH, importing the substance from China, selling it via the Internet for a profit, and intentionally failing to report the business activity and the income derived therefrom, the government respectfully submits that the defendant is dangerously close to the line here, engaging in conduct which could justify the Court refusing to grant any downward adjustment for acceptance of responsibility in this case.

If the Court denies the reduction in defendant's offense level for acceptance of responsibility and sentences him at Level 18, the government will withdraw the request for an upward departure or variance. Otherwise, the government respectfully submits that defendant's involvement with the importation, distribution and sale of JWH while on bond in this case, coupled with his failure to report the activity to the Presentence Report writer, warrants an upward departure of at least 3 levels, to a sentencing range of 27-33 months, or higher.

IV. APPLICATION OF §3553(a) FACTORS

A. Nature and Circumstances of the Offense and History and Characteristics of the Defendant

The defendant's offense of conviction, computer fraud and trafficking in unauthorized access devices, are non-violent offenses. This is taken into consideration by the advisory Sentencing Guidelines in calculating the offense level. However, as shown above, the defendant's conduct here was more egregious and far more serious that is reflected in the Sentencing Guidelines computation. He searched out, identified and compromised thousands of computers around the globe, for inclusion in his army of robot zombies. Defendant's activity was not merely idle curiosity or an educational exercise, since the evidence reflects that after seeking out and infecting thousands of computer systems or networks, defendant then utilized these "bot net zombies" to initiate and launch numerous cyber attacks on computer systems, networks and websites around the world, causing damage and otherwise interfering with the legitimate operation and use of these networks, including taking the entire University of Akron computer network off-line for over 8 hours in 2007.

Defendant possessed the knowledge, skills and the sophisticated software tools to accomplish this, and based upon a review of the IRC chat logs in which

defendant discussed his activities, defendant was absolutely without remorse for any of his conduct, lied to UA law enforcement authorities when questioned early on about his activity, attempted to conceal evidence on a DVD+R disk which he hid in the hallway of his dormitory, and bragged and boasted about his exploits while chatting with other individuals on the Internet. Indeed, as recently as February 2010, the defendant was still "bragging" about his exploits in postings on an Internet forum / discussion board, without any hint of remorse or regret for his conduct in this case.

Despite waiving indictment and pleading guilty to two federal felony offenses, defendant has continued to violate or "skirt" the law by operating an Internet website selling and distributing JWH, a synthetic form of marijuana THC, misrepresenting his employment status, income and activities to the Probation Office by failing to disclose this for-profit, commercial activity during the Presentence Investigation, and has continued to grow and use marijuana, as shown by his numerous postings on "grasscity.com" between 2008 and 2010.

For the foregoing reasons, the government respectfully submits that the Court should impose a sentence which is longer than the sentence called for at Offense Level Criminal History Category I (18-24 months), and should sentence the defendant within the range of 27-33 months, or higher, in this case.

B. Need for the Sentence Imposed to Reflect Seriousness of Offense, to Promote Respect for the Law and to Provide Just Punishment for the Offense

A sentence within the advisory guidelines range of 27-33 months of imprisonment, or higher, would promote respect for the law in this case. Although the defendant has no prior criminal history, the extent and seriousness of his conduct coupled with recently discovered evidence that the defendant has been engaged in the importation, sale and distribution of JWH, that he failed to disclose this for-profit commercial activity to the Presentence Report writer, and his apparent lack of remorse or regret for his hacking activities, weighs in favor of a sentence higher than 18-24 months in this case.

Based upon all of the foregoing reasons, the government respectfully submits that a sentence higher than the guidelines sentence of 18-24 months is warranted and should be imposed by the Court here, specifically, a sentence within the range of 27-33 months, or higher.

C. The Need to Afford Adequate Deterrence and to Protect the Public from Further Crimes of the Defendant

Based upon the defendant's conduct while on bond in this case, the government believes that this defendant is likely to engage in additional criminal conduct in the future. As such, a sentence higher than the guidelines sentence of 18-24 months is necessary to afford significant public deterrence. The government respectfully submits that 27-33 months, or higher, would be a more appropriate sentencing range.

Additionally, because of the defendant's extensive knowledge and experience in with computers, hacking techniques, creation and use of malicious computer software and codes, computer system vulnerabilities, and methods commonly employed to hide or mask computer intrusions, the government submits that strict and all-encompassing post-release conditions be placed upon the defendant following his release from prison, including computer and premises search provisions, as well as keystroke monitoring of any computer owned, possessed or otherwise used by the defendant.

V. CONCLUSION

For the reasons set forth above, the United States respectfully requests that the Court depart upward from the offense level set forth in the Presentence Report and impose a sentence of 27-33 months, or higher, in this case.

Respectfully submitted,

STEVEN M. DETTELBACH
United States Attorney

By: /s/ Robet W. Kern
Robert W. Kern (0005161)
Assistant U.S. Attorney
Suite 400, U.S. Courthouse
801 West Superior Avenue
Cleveland, Ohio 44113
Tel. No. (216) 622-3836
Fax No. (216) 522-2403
E-Mail: robert.kern@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on August 12, 2010, a copy of the foregoing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. All other parties will be served by regular U.S. Mail. Parties may access this filing through the Court's system.

/s/ Robert W. Kern
Robert W. Kern
Assistant U.S. Attorney